Docket No.: 58895/P003US/10305848
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert E. Cavanaugh
Appellant

Application No.: 10/727,068 | Confirmation No.: 5018

Filed: December 3, 2003 | Art Unit: 2135

For: SYSTEM AND METHOD FOR NETWORK EDGE DATA PROTECTION | Appellee: T. B. Truong

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

As required under 37 C.F.R. § 41.37(a), this brief is filed within two months from the Notice of Appeal filed in this case on February 2, 2009, and is in furtherance of said Notice of Appeal.

The fees required under 37 C.F.R. § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Deep Nines, Inc.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 43 claims pending in application.

B. Current Status of Claims

1. Claims canceled: 0
2. Claims withdrawn from consideration but not canceled: 0
3. Claims pending: 1-43
4. Claims allowed: 0
5. Claims rejected: 1-43

C. Claims On Appeal

The claims on appeal are claims 1-43

IV. STATUS OF AMENDMENTS

A Final Office Action (hereinafter "Final Action") rejecting the claims of the present application was mailed September 2, 2008. In response, Appellant did not file an Amendment After Final Rejection, but instead filed a Notice of Appeal, which this Brief supports. Accordingly, the claims on appeal are those filed in Appellant's response dated June 6, 2008. A complete listing of the claims is provided herewith in the Claims Appendix.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings and their reference characters, as required by 37 C.F.R.

§ 41.37(c)(1)(v). It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Embodiments of a system for providing protection against malicious code, such as in claim 1, are described, by way of example, in paragraphs [0027]-[0029], [0032]-[0033], and [0037]-[0038] and FIGURES 1 and 2. Paragraphs [0027]-[0029] and FIGURES 1 and 2 show the system comprises a malicious code analyzer (e.g., FIGURE 1, element 108; 9:29-10:3 (paragraph [0029])) disposed in a communication system traffic pattern between an originator of an information communication (e.g., Fig. 1, element 107; 9:12-14 (paragraph [0027])) of the communication system traffic pattern and an intended recipient of the information communication (e.g., Fig. 1, element 101; 9:10-12 (paragraph [0027])) to intercept the information communication (e.g., 12:21-13:17 (paragraphs [0037]-[0038])) and analyze the information communication for malicious code (e.g., 9:28-10:8 (paragraph [0029]); 15:21-16:4 (paragraph [0045])). Paragraphs [0032]-[0033] show the malicious code analyzer being configured to be transparent to systems of the communication system (e.g., 10:29-11:24 (paragraphs [0032]-[0033])).

Embodiments of a computer program product having a computer readable medium having computer program logic recorded thereon for providing protection against malicious code, such as in claim 13, are described, for example in paragraphs [0028]-[0029], [0031], and [0034]-[0036] and FIGURES 1 and 2. By way of example, paragraphs [0028]-[0029] show code for analyzing malicious code present in information communication traffic between an originator of an information communication of the communication traffic and an intended recipient of the information communication (e.g., 9:18-10:8 (paragraphs [0028]-[0029]); Fig. 1, element 108; Fig. 2, element 108). Paragraphs [0031] and [0034]-[0036] by way of example, show the computer program product further comprises code for steering the information communication between interfaces associated with the information communication originator and the intended recipient (e.g., 10:27-28 (paragraph [0031])) and providing a translate function which detours at least a portion of the information communication to the code for analyzing malicious code (e.g., 11:25-31 (paragraph [0034])) and which renders the code for analyzing malicious code invisible to the information

communication originator and the intended recipient (e.g., 12:1-20 (paragraphs [0035]-[0036])).

Embodiments of a method for providing protection against malicious code, such as in claim 20, are described, for example, in paragraphs [0037]-[0038] and [0040]. By way of example, paragraphs [0037]-[0038] show the method comprises intercepting packets in an information communication traffic pattern (e.g., 12:21-13:17 (paragraphs [0037]-[0038])). Paragraphs [0037]-[0038], for instance, show the method further comprises steering the packets between interfaces associated with an information communication originator and the intended recipient (e.g., 12:21-13:17 (paragraphs [0037]-[0038])), the steering providing detouring of at least a portion of the packets to a malicious code analyzer (e.g., 12:28-13:17 (paragraph [0038])). Paragraphs [0038], [0040], for example, show the method further comprises analyzing the at least a portion of the packets by the malicious code analyzer before releasing the at least a portion of the packets back into the traffic pattern (e.g., 12:28-13:17 (paragraph [0038]); 13:28-14:8 (paragraph [0040])).

Embodiments of a system for providing protection against malicious code, such as in claim 30, are described for example, in paragraphs [0028], [0031], [0033]-[0034], [0037]-[0038], and [0044] and FIGURES 1 and 2. By way of example, paragraphs [0028], [0031], [0034], and [0037] and FIGURES 1 and 2 show the system comprises a steering module for directing packets between a first interface and a second interface of the system (e.g., 9:18-27 (paragraph [0028]); 10:23-28 (paragraph [0031]); Fig. 1, element 104; Fig. 2, element 104), wherein the steering module provides a translate function that monitors each packet provided to the first interface and the second interface for packets to be provided malicious code analysis and directs at least some of the packets to a malicious code analyzer (e.g., 10:23-28 (paragraph [0031]); 11:25-31 (paragraph [0034]); 12:21-27 (paragraph [0037])). Paragraphs [0031], [0033], and [0038] and FIGURES 1 and 2 show the system further comprises the malicious code analyzer coupled to the steering module (e.g., 10:23-28 (paragraph [0031]); Fig. 1, element 108; Fig. 2, element 108) for receiving packets which are not addressed for receipt by the malicious code analyzer (e.g., 11:14-24 (paragraph [0033])) but which are directed to the malicious code analyzer by the steering module (e.g., 11:14-24 (paragraph [0033])) and for providing packets analyzed by the malicious code analyzer to the steering module (e.g., 12:28-13:17 (paragraph [0038]); Fig. 1, element 115). By way of example,

paragraph [0044] shows that the malicious code analyzer provide malicious code remediation (e.g., 15:10-19 (paragraph [0044])).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

- Claims 13-19 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.
- Claims 1, 3, and 8-11 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,780 (herein after *Muttik*) in view of U.S. Patent No. 7,096,501 (hereinafter *Kouznetsov*).
- Claim 10 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Kouznetsov* and further in view of U.S. Patent No. 7.203,192 (hereinafter *Desai*).
- Claims 13-14, 16-22, 26-34, and 40-43 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Desai*.
- Claims 2, 4-7, and 12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Kouznetsov* and further in view of U.S. Patent No. 7,032,005 (hereinafter *Mathon*).
- Claims 15, 23-25, and 35-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Desai* and further in view of *Mathon*.

VII. ARGUMENT

A. Statements Made by the Office in Response to Appellant's Arguments

In responding to Appellant's arguments filed June 6, 2008, the Office made several statements that are both incorrect and have no bearing on determining whether the claims are obvious under 35 U.S.C. § 103. Although these statements should have no impact on the Board's decision, Appellant addresses these statements in an abundance of caution to ensure no issues are waived.

Appellant takes issue with several statements made by the Office in responding to Appellant's arguments in response to the rejections under 35 U.S.C. § 103. First, the Office states:

> [A]pplicant recited the language, "between an originator of an information communication of said communication system traffic pattern and an intended recipient", where an originator does not clearly support anywhere by the specification, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter regards as the invention.

Final Action, pg. 2. The Office's assertion that the claimed "originator of an information communication" is new matter is incorrect. The recited claim language was included in the application as originally filed. The Office's assertion that "an originator" is not clearly supported by the specification is also incorrect. The claimed "originator of an information communication" is clearly supported by the specification – for example, at paragraphs [0027]-[0028].

The Office also states:

> [A]pplicant recited the language, "malicious code analyzer being configured to be transparent to systems of said communication system," wherein transparent to systems does not clearly support by the specification, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Final Action, pg. 2. The Office's assertion that the claimed "malicious code analyzer being configured to be transparent to systems of said communication systems" is new matter is incorrect. This portion of claim 1 was included in original claim 1. This portion of claim 1 is also supported by the specification – for example, at paragraphs [0032] and [0035].

B. 35 U.S.C. § 101 Rejections

Claims 13-19 stand rejected under 35 U.S.C. § 101 as being directed to nonstatutory subject matter.

1. Claim 13

The rejection of claim 13 states:

> With regard to claim 13, the computer program product having a computer readable medium having computer program is not clearly define any where in the specification, which is construed as a "new matter" and failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Moreover, the claimed language direct clearly toward a computer program, which is not patentable

Office Action, pg. 2. The Office has not shown that claim13 is directed to nonstatutory subject matter.

As an initial matter, it unclear why the Office insists on construing the claimed "computer program product" as new matter. Claim 13 has not been amended and was listed

as a claim when the present application was filed. *See* MPEP 608.01(I) (2008) ("In establishing a disclosure, applicant may rely not only on the description and drawing as filed but also on the original claims . . . .). Moreover, whether claim 13 presents new matter has no bearing on the determination of whether the claim is directed to nonstatutory subject matter under 35 U.S.C. § 101. It is also unclear why the Office continues to assert that claim 13 fails to particularly point out and distinctly claim which the Appellant regards as the invention. This argument, which quotes 35 U.S.C. § 112, has no bearing on whether claim 13 is directed to nonstatutory subject matter under 35 U.S.C. § 101.

Moreover, the Office's assertion that computer programs are not patentable is incorrect. It has been USPTO practice for a number of years that "Beauregard Claims," such as claim 13, are statutory as product claims. *See* MPEP 2106.01(I). This practice is consistent with *In re Nuijten*, 500 F.3d 1346 (Fed. Cir. 2007) and *In re Lowery*, 32 F.3d 1583 (Fed. Cir. 1994). In addition, these claims satisfy the machine-or-transformation test described by the Federal Circuit in *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008). Under the machine-or-transformation test, a process is patent eligible if (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing. *Id.* at 961-62.

Claim 13, which recites a computer program product comprising "code for analyzing malicious code present in information communication traffic" and "code for steering information communications" is necessarily tied to a machine. The claimed code cannot be separated from the machine on which it is run. For at least this reasons, claim 13 satisfies the machine-or-transformation test. Claims 14-19 are rejected based on the same rational as claim 13. Final Action, pg. 2. Like claim 13, claims 14-19 are necessarily tied to a machine and, therefore, satisfy the machine-or-transformation test. Appellant respectfully requests that the Board reverse the rejections of claims 13-19 under 35 U.S.C. § 101.

C. The 35 U.S.C. § 103 Rejections

The test for non-obvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in *Graham v. John Deere and Co.*, 383 U.S. 1 (1966) set forth

the factual inquiries which must be considered in applying the statutory test: (1) determining of the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art. As discussed further hereafter, Appellant respectfully asserts that the claims include non-obvious differences over the cited art.

As discussed further below, the rejections under 35 U.S.C. § 103(a) should be withdrawn because, when considering the scope and content of the applied references, there are significant differences between the applied combinations and claims 1-43, as the applied combinations fail to disclose all elements of these claims. Considering the lack of disclosure in the applied combinations of all elements of claims 1-43, one of ordinary skill in the art would not find claims 1-43 obvious under 35 U.S.C. §103. The rejections should be reversed for at least for this reason.

In addition, the Office has not shown that a person of ordinary skill in the art would have been motivated to make applied combinations. *See In re Kahn, 441 F.3d 977, 986 (Fed. Cir. 2006); MPEP § 2143.01 (2008).* The rejections under 35 U.S.C. § 103(a) should also be reversed because the Office has not provided an articulated reasoning with a rational underpinning to support its conclusions of obviousness. *See KSR Int'l Inc. v. Teleflex Co.*, 127 S.Ct. 1727, 1741 (Fed. Cir. 2007) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."); MPEP § 2142 (2008). For all of these reasons, Appellant respectfully requests that the Board reverse the rejections of claims 1-43 under 35 U.S.C. § 103(a).

1. The Rejections of Claims 1, 3, and 8-11 under 35 U.S.C. § 103 over *Muttik* in view of *Kouznetsov*

Claims 1, 3, and 8-11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Kouznetsov*.

a. Independent Claim 1

The combination of *Muttik* and *Kouznetsov* does not render claim 1 obvious because the applied combination does not disclose every element of claim 1. In addition, the Office has not shown that a person of ordinary skill would have been motivated to combine *Muttik*

and *Kouznetsov*. Moreover, the Office has not articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. Appellant respectfully requests that the Board reverse the rejection of claim 1.

i. Muttik in view of Kouznetsov fails to teach a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication and an intended recipient of said information communication to intercept said information communication

Claim 1 recites "a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient of said information communication." The cited combination of *Muttik* and *Kouznetsov* does not teach at least this feature of claim 1. To aid the Board in understanding the foregoing feature of claim 1, attention is directed to the Present Application at Figure 1 and paragraphs [0027]-[0028]. Paragraph [0028] explains that "The illustrated embodiment disposes a protective system or systems of the present invention in the traffic pattern between real client 101 and real server 107." Present Application, para. [0028] (emphasis added).

The Office alleges that the claimed "analyzer disposed in a communication traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient of said information communication" is disclosed by *Muttik*, specifically at Figure 2, element 108, and column 1, line 65, through column 2, line 11. Final Action, pg. 7. It appears that the rejection relies upon the emulator of *Muttik* to teach the claimed malicious code analyzer. Without admitting that such characterization is correct, it is noted that *Muttik* does not disclose the location of the emulator in a communications system traffic pattern between an originator and a recipient.

Instead, *Muttik* discloses a system in which an emulator stored and run on a computer system is used to analyze computer code that is received by the computer system. *Muttik*, Fig. 1, 1:65-2:11 ("The system operates by emulating the software within an insulated environment in a computer system so that the computer system is insulated from malicious actions of the software.") (emphasis added). The emulator disclosed in *Muttik* analyzes software, or code, only after the code has been received by the computer system. *See, e.g.,*

Muttik, 3:30-53. After receiving code, and before executing the code, the "computer system 106 uses emulator 110 to analyze code 108 in order to detect malicious behavior . . . ." *Muttik*, 3:49-50. *Muttik*, therefore, discloses a system in which a software emulator is disposed at a recipient of computer code not between an originator of an information communication and an intended recipient of said information communication, as required by claim 1.

The Office does not rely on *Kouznetsov* to teach or suggest "a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient," as recited by claim 1. *See* Final Action, pp. 3-4, 7-8. Nor does it appear that the cited portions of *Kouznetsov* teach or suggest such feature. In fact, *Kouznetsov* discloses a system in which an "anti-malware scanner" is installed and run on a mobile wireless device. *See, e.g., Kouznetsov*, 3:25-50. That is, *Kouznetsov* discloses a system in which an anti-malware scanner is disposed at a recipient of a communication (a mobile wireless device) not between an originator of an information communication and an intended recipient of said information communication, as required by claim 1.

The combination of *Muttik* and *Kouznetsov* does not render claim 1 obvious at least because the references do not disclose "a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient of said information communication."

ii. Muttik in view of Kouznetsov fails to teach a malicious code analyzer being configured to be transparent to systems of said communication system

The proposed combination of *Muttik* and *Kouznetsov* also fails to disclose the portion of claim 1 that recites "said malicious code analyzer being configured to be transparent to systems of said communication system." The Office admits that this feature is not taught or suggested by *Muttik*, but asserts that *Kouznetsov* discloses the feature. Final Action, pg. 7. The Office's reliance on *Kouznetsov* is misplaced. The cited portion of *Kouznetsov* states that its "on-access scanner 702 may be entirely transparent to the user until malicious code is discovered." *Kouznetsov*, 13:22-25. That a scanner is transparent to a user, however, does

not mean that the scanner is "transparent to systems of said communication system," as required by claim 1. In fact, *Kouznetsov* expressly discloses that its "anti-malware scanner" is visible to systems in the disclosed wireless network.

Kouznetsov discloses a an anti-malware scanner for a mobile wireless device. *Kouznetsov*, 3:37-44. The disclosed scanner communicates with the wireless device's operating system. *See, e.g., Kouznetsov*, 5:45-50, 13:63-65 ("in case an infected file is opened, the hooking application must indicate to the operating system that this event should not traverse further in the file system"). *Kouznetsov's* disclosed anti-malware scanner is, therefore, at least visible to the mobile wireless device on which the scanner resides. Additionally, the disclosed anti-malware scanner is visible to server-side systems (also called back-end architecture) in the wireless network disclosed by *Kouznetsov*. *See, e.g., Kouznetsov*, 3:45-56.

Claim 1 is not obvious in view of the combination of *Muttik* and *Kouznetsov* at least because the references do not disclose the portion of claim 1 that recites "said malicious code analyzer being configured to be transparent to systems of said communication system."

iii. *A person of ordinary skill would not have been motivated to combine Muttik and Kouznetsov*

The rejection of claim 1 fails to set forth a *prima facie* case of obviousness because the rejection is not supported by evidence that a person of ordinary skill would have been motivated to combine *Muttik* and *Kouznetsov*. The rejection of record states that "[t]he ordinary skilled person would have been motivated to: (1) have modified the invention of Muttik with the teaching of Kouznetsov to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software." Final Action, pg. 8. This is not a motivation to combine *Muttik* and *Kouznetsov*. It is the exact problem that *Muttik* claims to address. *See Muttik*, 1:59-63. *Muttik* addresses the alleged motivation cited in the rejection of record; therefore, a person of ordinary skill would not have been motivated to look beyond *Muttik* to address the alleged motivation cited by the Final Action.

Moreover, a person of ordinary skill would not have been motivated to combine *Muttik* and *Kouznetsov* because they teach away from disposing a malicious code analyzer

"in a communication system traffic pattern between an originator of an information communication of said communication systems traffic pattern and an intended recipient of said information communication." *See, e.g., In re Grasselli*, 713 F.2d 731, 743 (Fed. Cir. 1983) (it is improper to combine references where the references teach away from their combination). In this case, Appellant disposes a malicious code analyzer in a communication system traffic pattern between an originator of an information communication and an intended recipient of said information communication to intercept said information communication. As discussed above, *Muttik* and *Kouznetsov* teach systems in which a malicious code analyzer is disposed at a recipient of computer code. *Muttik* and *Kouznetsov*, therefore, teach away from the claimed invention because they suggest a system in which a malicious code analyzer is disposed at a recipient. *See, e.g., In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994) ("A reference may be said to teach away when a person of ordinary skill, upon reading the reference . . . would be led in a direction divergent from the path that was taken by the applicant.").

Because the Office has failed to provide evidence that a person of ordinary skill would have been motivated to combine *Muttik* and *Kouznetsov*, the Appellee has failed to make a *prima facie* case of obviousness.

iv. The Office has not clearly articulated why the claimed invention would have been obvious

The rejection of claim 1 is at odds with the Supreme Court's requirement that obviousness rejections be supported by clearly articulated reasoning with some rational underpinning. *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007). In rejecting claim 1, the Office does not even attempt to explain how a person of ordinary skill could have combined the teachings of *Muttik* and *Kouznetsov* to arrive at the claimed invention.

This is not a situation where familiar elements are combined according to known elements. *See, e.g., KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1731 (2007). The Office has provided no explanation for how or why a person of ordinary skill would have modified an emulator that resides on a computer (*Muttik*) and a malware scanner for a mobile wireless device (*Kouznetsov*) to arrive at a system for providing protection against malicious code that is "disposed in a communication traffic pattern between an originator of an information communication . . . and an intended recipient of said information communication to intercept

said information communication and to analyze said information communication." As pointed out above there are significant differences between the claimed invention and the cited references. Mainly, *Muttik* and *Kouznetsov* do not disclose "a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication . . . and an intended recipient" and do not disclose a "malicious code analyzer being configured to be transparent to systems of said communication system." Even using hindsight analysis with the present application as a road map, it unclear to Appellant how *Muttik* and *Kouznetsov* could be modified and combined to reach the claimed invention.

b. Dependent Claims 3 and 8-11

Dependent claims 3 and 8-11 each depend from independent claim 1 and inherit all of the limitations of claim 1. It has been shown above that claim 1 is not obvious in view of *Muttik* and *Kouznetsov*. The rejections of claims 3 and 8-11 do not cure the above identified deficiencies in the rejection of claim 1. Claims 3 and 8-11 are, therefore, allowable at least for their dependence from claim 1. Moreover, claims 3 and 8-11 recite features that make them patentable on their own.

i. Dependent Claim 3

Claim 3 recites, in part, "a translate function that monitors each packet provided to an interface of said system for packets to be provided malicious code analysis by said malicious code analyzer." The Office asserts that this feature of claim 3 is disclosed by *Muttik* at column 1, lines 40-47, and column 3, line 65, through column 4, line 11. Final Action, pg. 8. The cited portions of *Muttik* merely disclose that a program's system calls can be analyzed to determine whether the program is likely to exhibit malicious behavior. *Muttik*, 1:40-47, 3:65-4:11.

Analyzing a program's system calls to determine whether a program is likely to exhibit malicious behavior does not teach or suggest the claimed "translate function." The translate function of claim 3 "monitors each packet provided to an interface of said system for packets to be provided malicious code analysis." *Muttik* does not disclose a system in which packets provided to an interface are monitored. As discussed above, *Muttik* discloses a system in which computer code that is introduced to a computer system is emulated before it

is executed by the computer system. *Muttik*, 3:23-53. Nothing in *Muttik* suggests that the disclosed emulator monitors packets at an interface of the disclosed system.

Claim 3 is not obvious in view of the combination of *Muttik* and *Kouznetsov* at least because the references do not disclose the portion of claim 3 that recites "a translate function that monitors each packet provided to an interface of said system for packets to be provided malicious code analysis by said malicious code analyzer." Moreover, the Office has provided no explanation for why a person of ordinary skill would have found claim 3 obvious given the differences between the cited references and the claimed invention. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). For at least the reasons discussed in this section, Appellant respectfully requests that the Board reverse the rejection of claim 3.

ii. *Dependent Claim 11*

The combination of *Muttik* and *Kouznetsov* does not teach or suggest the portion of claim 11 that recites "a communications throttle for determining if said information communication is to be passed by said system." The rejection of record states that *Muttik* discloses this feature. Final Action, pg. 8. The citation of *Muttik* as disclosing the aforementioned portion of claim 11 is nonsensical because, as discussed above, the emulator disclosed by *Muttik* is not disposed in a communication system traffic pattern between an originator of an information communication and an intended recipient of the information communication to intercept the information communication. *Muttik* does not determine if an information communication should be passed because the disclosed emulator resides on an information communication recipient, not in a communication systems traffic pattern. The portion of *Muttik* cited by the Office merely discloses that the results of code analysis are reported. *Muttik*, 4:8-11, fig. 3, element 314. The Office's argument that reporting the results of emulation meets the claimed "determining if said information communication is to be passed by said system" is incorrect.

The rejection does not rely on *Kouznetsov* to teach or suggest the feature, nor do the cited portions of *Kouznetsov* appear to teach or suggest the feature. Therefore, the above-

recited feature is not taught by the cited combination of references. Moreover, the Office has made no attempt to explain why the invention of claim 11 would have been obvious given the differences between the cited references and claimed invention. For at least these reasons, claim 11 is not obvious. Appellant respectfully requests that the Board reverse of the rejection of claim 11.

2. The Rejection of Claim 10 under 35 U.S.C. § 103 over *Muttik* in view of *Kouznetsov*, and further in view of *Desai*

Claim 10 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Kouznetsov* and further in view of *Desai*. Final Action, pg. 9. Dependent claim 10 depends directly from independent claim 1 and, thus, inherits all of the limitations of claim 1. As discussed above, the cited combination of *Muttik* and *Kouznetsov* does not teach or suggest all limitations of claim 1. The cited combination of *Muttik* and *Kouznetsov*, therefore, does not teach or suggest all the claim limitations of claim 10. The rejection of record does not rely on *Desai* to cure the deficiencies of *Muttik* and *Kouznetsov* with respect to claim 1, nor does *Desai* cure those deficiencies. It is respectfully submitted that dependent claim 10 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 10 also presents subject matter that makes it patentable on its own. For example, claim 10 recites, in part, "a steering module for said information communication between a first interface and a second interface of said system . . . ." The Office argues that claim 10 has similar limitations as claim 3, and is therefore rejected for similar reasons. Final Action, pg. 9. However, claim 3 does not require a steering module nor does claim 3 require the direction of at least some of the information communication to the malicious code analyzer. Therefore, the Office's assertion that the claims contain similar limitations is incorrect. Further, the sections of *Muttik* cited in the rejection of claim 3, and asserted as being relevant to claim 10, do not disclose a steering module between a first and a second interface of the system. The rejection does not rely on *Kouznetsov* to teach or suggest the feature, nor do the cited portions of *Kouznetsov* appear to teach or suggest the feature. Therefore, the above-recited feature of claim 10 is not taught by the cited combination of *Muttik* and *Kouznetsov*.

The Office also asserts that *Desai* teaches the claimed "steering module." Final Action, pg. 9. *Desai* discloses a method for steering a network packet from a network interface module to a processing resource. *Desai*, 4:36-51. The method involves associating a unique identifier with a processing resource and pushing the identifier to a network interface, such as a Netmod. *Desai*, 5:24-40. When a network data packet is then received at the interface, the assigned processing resource is determined and the network data packet is steered to the appropriate processing resource. *Id.*

The rejection of record does not disclose what portions of *Desai* the Office believes are analogous to the claimed "first interface" and the claimed "second interface." But it does not appear to Appellant that *Desai* discloses a system with a steering module that "provides a translate function that monitors each information communication provided to said first interface and said second interface for information communication to be provided malicious code analysis. *Desai* merely discloses that packets received at a single network interface – a Netmod - are analyzed and directed to an appropriate processing resource. That is, *Desai* discloses a system in which information communications are monitored at a single interface, not a "first interface" and "second interface," as required by claim 10.

The rejection of record also fails to explain why a person of ordinary skill would have been motivated to combine *Desai* with *Muttik* and *Kouznetsov*. The Office asserts that a person of ordinary skill would have been motivated to combine "the modified invention of Muttik with the teaching of Desai to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software." As noted above, this is not a motivation to combine *Muttik*, *Kouznetsov*, and *Desai*. It is the exact problem that *Muttik* claims to address. *See Muttik*, 1:59-63.

Moreover, the Appellee has provided no explanation for how the completely dissimilar systems of *Muttik*, *Kouznetsov*, and *Desai* could be modified and combined to arrive at the claimed invention. *Muttik* discloses an emulator "within an insulated environment in a computer system so that the computer system is insulated from malicious actions of the software." *Muttik*, 2:2-5. *Desai* discloses Netmods for directing packets to processing resources. *Desai*, abstract. And *Kouznetsov* discloses an anti-malware scanner for use on a mobile wireless device. *Kouznetsov*, abstract. The Office's proposed

combination is not an instance where familiar elements are combined according to known methods. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1739 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). Even if the cited references disclosed every claim limitation, which they do not, the proposed combination would require substantial operational changes to the systems of *Muttik*, *Kouznetsov* and *Desai* due to their disparate features and disparate places wherein the systems reside. And it is well settled that a proposed modification of prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *See, e.g., In re Ratti*, 270 F.2d 810 (CCPA 1959); MPEP § 2143.01(VI) (2008).

Claim 10 is not obvious because the proposed combination of *Muttik*, *Kouznetsov*, and *Desai* does not teach or suggest every claim limitation of claim 10. Moreover, the Office has not shown that a person of ordinary skill would have been motivated to make the proposed combination, and the rejection of claim 10 is not supported by an explanation for why the claimed invention would have been obvious. Appellant respectfully requests that the Board reverse the rejection of claim 10.

3. The Rejections of claims 13-14, 16-22, 26-34, and 40-43 under 35 U.S.C. § 103(a) over *Muttik* in view of *Desai*

Claims 13-14, 16-22, 26-34, and 40-43 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Desai*. Final Action, pg. 9.

a. Independent Claim 13

The rejection of claim 13 states:

> This claim consists of a computer program having a computer readable medium having computer program logic recorded thereon for providing protection against malicious code to implement claims 1 (without the transparency) and 10; thus it is rejected with the same rationale applied against claims 1 (without the transparency) and 10 above.

Final Action, pp. 9-10. As an initial matter, Appellant disputes the Office's characterization of claim 13. Claim 13 is not computer program to implement claims 1 and 10. Claim 13 is a separate embodiment of the invention that has its own unique features. By relying on the

rejections of claims 1, and 10, rather than examining the claim, the Office attempts to improperly shift the burden of making a *prima facie* case onto Appellant. Appellant respectfully requests that the Board reverse the rejection of claim 13 and require the Office to make a case of obviousness consistent with Supreme Court precedent in *Graham* and *KSR*.

The rejection of claim 13 fails at least because the combination of *Muttik* and *Desai* does not teach or suggest every limitation of claim 13, because a person of ordinary skill would not have been motivated to combine *Muttik* and *Desai*, and because the Office has not articulated a reason with some rational underpinning to support its conclusion of obviousness.

i. *The proposed combination of Muttik and Desai does not teach code for analyzing malicious code present in information communication traffic between an originator of an information communication and an intended recipient of said information communication*

Claim 13 recites, in part, "code for analyzing malicious code present in information communication traffic between an originator of an information communication of said communication traffic and an intended recipient of said information communication." The Office apparently asserts that this portion of claim 13 is disclosed by *Muttik* – specifically, figure 2, element 108, and column 1, line 65, through column 2, line 11. Final Action, pp. 7, 9-10 (rejections of claims 1, 10, and 13). As discussed above, with respect to claim 1, *Muttik* discloses a system in which code is analyzed at a recipient of code, not "between an originator of an information communication and an intended recipient of said information communication," as required by claim 13. Thus, *Muttik* does not disclose the claimed "code for analyzing malicious code present in information communication traffic between an originator of an information communication of said communication traffic and an intended recipient of said information communication." Moreover, The Office does not rely on *Desai* as disclosing this portion of claim 13; nor do the cited portions of *Desai* disclose this portion of claim 13.

The combination of *Muttik* and *Desai* does not render claim 13 obvious at least because the references do not disclose "code for analyzing malicious code present in information communication traffic between an originator of an information communication of said communication traffic and an intended recipient of said information communication."

ii. The proposed combination does not teach a translate function which renders said code for analyzing malicious code invisible to said information communication originator and said intended recipient.

Claim 13 recites also recites "a translate function . . . which renders said code for analyzing malicious code invisible to said information communication originator and said intended recipient." As an initial matter, the Office has not presented evidence that any portion of *Muttik* or *Desai* discloses the aforementioned portion of claim 13. The Office argues that claim 13 is "rejected with the same rationale applied against claims 1 (without the transparency) and 10 above." Final Action, pg. 10. Yet the Office relied on *Kouznetsov* to teach the portion of claim 1 related to transparency. In rejecting claim 13, the Office does not rely on *Kouznetsov* at all. *See* Final Action, pg. 10. Moreover, as discussed above with respect to claim 1, *Kouznetsov* does not teach or suggest transparency. No cited portion of *Muttik* or *Desai* discloses a translate function which renders said code for analyzing malicious code invisible to said information communication originator and said intended recipient. For at least this reason, claim 13 is not obvious in view of *Muttik* and *Desai*.

iii. *A person of ordinary skill would not have been motivated to make the proposed combination*

The rejection of record also fails to explain why a person of ordinary skill would have been motivated to combine *Muttik* and *Desai*. The Office asserts that a person of ordinary skill would have been motivated to "modify the modified-invention of Muttik with the teaching of Desai to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software." As noted above, this is not a motivation to combine *Muttik* and *Desai*. It is the exact problem that *Muttik* claims to address and, therefore, a person of ordinary skill would not have been motivated to look beyond *Muttik* to address the alleged motivation cited by the Office.

iv. *The rejection is not supported by a rational explanation*

The rejection of claim 13 is at odds with the Supreme Court's requirement that obviousness rejections be supported by clearly articulated reasoning with some rational underpinning. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead;, there

must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). The rejection of claim 13 is conclusory and does not even attempt to articulate how a person of ordinary skill could have modified and combined the teachings of *Muttik* and *Desai* to arrive at the claimed invention. For that matter, the Office has not even identified the level of skill in the art, a prerequisite to making any determination of obviousness. *Id.* at 1730.

The Office has provided no explanation for why or how a person of ordinary skill would have known methods to somehow modify an emulator that resides on a computer (*Muttik*) and network interfaces for directing network data packets from one network to processing resources (*Desai*) to arrive at the claimed computer program product. As pointed out above there are significant differences between the claimed invention and the cited references. The Appellee has provided no explanation for why a person of ordinary skill would have found it obvious to implement the claimed "code for analyzing malicious code present in information communication traffic" based on an emulator that resides within a computer system. Nor has the Office provided an explanation for why a person of ordinary skill would have found it obvious to implement the claimed "code for . . .providing a translate function . . .which renders said code for analyzing malicious code invisible to said information communication originator and said intended recipient" based on the proposed combination.

b. Dependent Claims 14 and 16-19

Dependent claims 14 and 16-19 each depend from independent claim 13 and inherit all of the limitations of claim 13. It has been shown above that rejection of claim 13 is deficient. The rejections of claims 14 and 16-19 do not cure the above identified deficiencies in the rejection of claim 13. Claims 14 and 16-19 are, therefore, allowable at least for their dependence from claim 13. Moreover, claims 14 and 16-19 recite features that make them patentable on their own.

i. Claim 18

The Office asserts that claim 18 has limitations that are similar to those of claim 3 and are rejected "with the same rationale applied against claim 3 above." Final Action, pg. 10. The Appellee, therefore, relies on *Muttik*, column 1, lines 40-47, and column 3, line 65,

through column 4, line 11, as disclosing the portion of claim 18 that recites "said translate function monitors each information communication provided to a first interface of said interfaces and a second interface of said interfaces for information communication to be provided malicious code analysis." *See* Final Action, pg. 8 (rejection of claim 3).

As an initial matter, Appellant disputes the Office's characterization of claim 18. Claim 3 recites "a translate function that monitors each packet provided to an interface of said system . . ." Claim 18 recites "wherein said translate function monitors each information communication provided to a first interface of said interfaces and a second interface of said interfaces . . ." The claims clearly recite distinct subject matter.

As discussed above, with respect to claim 3, *Muttik* does not disclose monitoring information communication provided to an interface. Moreover, as discussed with respect to claim 10, *Muttik* does not disclose monitoring a first and second interface. Claim 18 is not obvious at least because *Muttik* does not disclose the portion of claim 18 that recites "wherein said translate function monitors each information communication provided to a first interface of said interfaces and a second interface of said interfaces."

ii. Claim 19

The Office asserts that claim 19 has limitations that are similar to those of claim 11 and are rejected "with the same rationale applied against claim 11 above." Final Action, pg. 10. The Appellee, therefore, relies on *Muttik*, Figure 2, element 212, and column 4, lines 8-11, as disclosing the portion of claim 19 that recites "code for throttling communications by receiving information with respect to information communication and determining if said information communication is to be passed by said interfaces." *See* Final Action, pg. 8 (rejection of claim 11).

As discussed above, with respect to claim 11, *Muttik* does not disclose "determining if said information communication is to be passed by said system". For the same reasons, *Muttik* does not teach or suggest the portion of claim 19 that recites "determining if said information communication is to be passed by said interfaces."

c. Independent Claim 20

Claim 20 is not obvious in view of *Muttik* and *Desai* because the combination does not teach or suggest every limitation of claim 20 and a person of ordinary skill would not have been motivated to combine *Muttik* and *Desai*. Moreover, the Office has failed to articulate reasoning explaining why a person of ordinary skill would have found the claimed invention obvious in view of *Muttik* and *Desai*.

i. *The combination of Muttik and Desai does not disclose intercepting packets in an information communication traffic pattern*

Claim 20 recites, in part, "intercepting packets in an information communication traffic pattern." The Office asserts that this portion of claim 20 is disclosed by *Muttik* at column 4, lines 59-64, and column 5, lines 1-13. Final Action, pg. 10. The Office's reliance on *Muttik* is misplaced. *Muttik* does not disclose intercepting packets in an information communication traffic pattern. As discussed above, *Muttik* discloses a system for emulating computer code that has been received by a computer system. The cited portion of *Muttik* merely discloses an example set of system calls generated by code that may indicate suspicious behavior. *Muttik*, 4:59-5:13. Claim 20 is not obvious at least because the combination of *Muttik* and *Desai* does not disclose "intercepting packets in an information communication traffic pattern."

ii. *The proposed combination does not teach analyzing at least a portion of said packets by said malicious code analyzer before releasing said at least a portion of said packets back into said traffic pattern.*

Claim 20 also recites "analyzing said at least a portion of said packets . . . before releasing said at least a portion of said packets back into said traffic pattern." The Office asserts that *Muttik*, at column 3, lines 54-57, teaches or suggests this portion of claim 20. Final Action, pp. 10-11. The cited portion of *Muttik* merely states, "FIG. 2 illustrates the internal structure of emulator 110, which emulates and analyzer code 108 in order to detect malicious behavior in accordance with an embodiment of the present invention." *Muttik*, 3:54-57. As discussed above, *Muttik* merely discloses that "[t]he system then reports results of the analysis to a user of a computer system 106 (step 314)." *Muttik* does not discloses releasing packets into an information communication traffic pattern. The Office does not rely

on Desai to teach this feature, nor dies it appear that the cited portion of *Desai* teaches the feature. Claim 20 is not obvious because the proposed combination of *Muttik* with *Desai* does not disclose the portion of claim 20 that recites "analyzing said at least a portion of said packets . . . before releasing said at least a portion of said packets back into said traffic pattern."

iii. *A person of ordinary skill would not have been motivated to make the proposed combination.*

The Office has not shown that a person of ordinary skill would have been motivated to combine *Muttik* and *Desai*. The Office asserts that a person of ordinary skill would "have modified the modified-invention of Muttik with the teaching of Desai to detect malicious software without requiring manual analysis of the software by a human expert, and without exposing the computer system to potentially malicious actions of the software." Final Action, pg. 11. As discussed above, this is not a motivation to combine *Muttik* and *Desai*. This is the exact problem that *Muttik* claims to address. *Muttik*, 1:59-63. A person of ordinary skill would not have looked beyond *Muttik* to address the problem presented by the Office.

iv. *The Office has not articulated a rational basis for concluding that claim 20 is obvious in view of Muttik and Desai*

The rejection of claim 20 is conclusory and does not even attempt to articulate how a person of ordinary skill could have modified and combined the teachings of *Muttik* and *Desai* to arrive at the claimed invention. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.").

The Office has provided no explanation for why or how a person of ordinary skill would have known methods to somehow modify an emulator that resides on a computer (*Muttik*) and a network interfaces for directing network data packets from one network to processing resources (*Desai*) to arrive at the claimed method for protection against malicious code. As pointed out above there are significant differences between the claimed invention and the cited references. The Appellee has provided no explanation for why a person of

ordinary skill would have found it obvious to implement the claimed "intercepting packets in an information" based on an emulator that resides within a computer system. Nor has the Office provided an explanation for why a person of ordinary skill would have found it obvious to implement the claimed "analyzing said at least a portion of said packets by said malicious code analyzer before releasing said at least a portion of said packets back into said traffic pattern" based on the proposed combination. The rejection of claim 20 simply does not satisfy the requirements for proving obviousness set forth by the Supreme Court in *KSR*.

d. Dependent Claims 21-22 and 26-29

Dependent claims 21-22 and 26-29 each depend from independent claim 20 and inherit all of the limitations of claim 20. It has been shown above that *Muttik* in view of *Desai* does not meet the limitations of independent claim 20 and a person of ordinary skill would not have been motivated to combine *Muttik* and *Desai*. The rejections of claims 21-22 and 26-29 do not cure the above identified deficiencies in the rejection of claim 20. Claims 21-22 and 26-29 are, therefore, allowable at least for their dependence from claim 20. Moreover, claims 21-22 and 26-29 recite features that make them patentable on their own.

i. Claim 21

The Office argues that claim 21 "has limitations that is [sic] similar to those of claim 20, thus it is rejected with the same rational applied against claim 20 above." Final Action, pg. 11. Yet claim 21 recites "disposing a protective system providing said intercepting, steering, and analyzing in a network link between said information communication originator and said intended recipient." This feature of claim 21 is not recited by claim 20. The rejection of record fails because obviousness must be determined based on the invention "as a whole," and the Office completely ignores the aforementioned limitation of claim 21. *See* 35 U.S.C. § 103(a) ("A patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious . . . ."). In rejecting, claim 21 the Offices failed to provide any evidence that the proposed combination of *Muttik* and *Desai* teaches or suggests "disposing a protective system providing said intercepting, steering, and analyzing in a network link between said information communication originator and said intended recipient."

And, in fact, neither *Muttik* nor *Desai* teaches or suggests "disposing a protective system providing [the claimed] intercepting, steering, and analyzing in a network link between said information communication originator and said intended recipient." As discussed above, *Muttik* teaches disposing an emulator in a recipient of computer code. *Desai* merely discloses network interfaces (Netmods) for steering network data packets from a network to a processing resource. *See, e.g., Desai*, 4:27-35. Claim 21 is not obvious in view of the proposed combination of *Muttik* and *Desai* at least because the proposed combination does not disclose the portion of claim 21 that recites "disposing a protective system providing said intercepting, steering, and analyzing in a network link between said information communication originator and said intended recipient." Moreover, the Office has offered no reason explaining why a person of ordinary skill would have found it obvious to disposing the claimed protective system in a network link between an information communication originator and an intended recipient. Appellant requests that the rejection of claim 21 be reversed.

ii. Claim 22

Claim 22 recites "wherein said protective system is disposed as a protected network edge device." The Office asserts that this portion of claim 22 is disclosed by *Muttik*, figure 1 and column 3, lines 22-53. Final Action, pp. 11-12. *Muttik* merely discloses an emulator that resides on a computer system. *Muttik*, Fig. 1, 3:22-53. Claim 22 is not obvious in view of the proposed combination of *Muttik* and *Desai* at least because the proposed combination does not disclose the portion of claim 22 that recites "wherein said protective system is disposed as a protected network edge device." Appellant respectfully requests that the Board reverse the rejection of claim 22.

iii. Claim 28

The Office asserts that claim 28 has "limitations that is [sic] similar to those of claim 3, thus they aer [sic] rejected with the same rationale applied against claim 3 above." As an initial matter, Appellant disputes the Office's assertion that claim 28 has similar limitations to claim 3. Claim 3 recites "a translate function that monitors each packet provided to an interface of said system for packets to be provided malicious code analysis by said malicious code analyzer." Claim 28 recites "monitoring each packet provided to a first interface and a

second interface for information to be provided malicious code analysis." The claims recite distinct subject matter.

Based on the rejection, it appears that the Office believes *Muttik* discloses the portion of claim 28 that recites "monitoring each packet provided to a first interface and a second interface for information to be provided malicious code analysis." *See* Final Action, pg. 8 (rejection of claim 3). As discussed above, *Muttik* does not monitor packets provided to any interface, much less each packet provided to a first interface and a second interface, as is required by claim 28. Thus, the Office's reliance on *Muttik* as disclosing the claimed "monitoring each packet provided to a first interface and a second interface for information to be provided malicious code analysis" is improper. Claim 28 is not obvious at least because the proposed combination of *Muttik* and *Desai* does not teach or suggest the claimed "monitoring each packet provided to a first interface and a second interface for information to be provided malicious code analysis." Appellant respectfully requests that the Board reverse the rejection of claim 28.

e. Claim 30

The rejection of claim 30 states: "This claim has limitations that is [sic] similar to those of claims 1 (without the transparency), 3, and 10, thus it is rejected with the same rationale applied against claims 1 (without the transparency), 3, and 10 above." Final Action, pg. 12. Appellant disputes the Office's characterization of claim 30. Claim 30 is a separate embodiment of the invention that has its own unique features. By relying on the rejections of claims 1, 3, and 10, rather than examining the claim, the Office attempts to improperly shift the burden of making a *prima facie* case onto Appellant. Appellant respectfully requests that the Board reject the rejection of claim 30 and require the Office to make a case of obviousness consistent with Supreme Court precedent in *Graham* and *KSR*.

Claim 30 is not obvious in view of the proposed combination of *Muttik* and Desai because the proposed combination does not meet every feature of claim 30, and a person of ordinary skill would not have been motivated to modify and combine the teachings of *Muttik* and *Desai* to arrive at the claimed invention. Additionally, the rejection of claim 30 is deficient because the Office has not articulated reasoning to support its legal conclusion of obviousness.

i. *The proposed combination does not teach a steering module that provides a translate function that monitors each packet provided to said first interface and said second interface for packets to be provided malicious code analysis*

The Office apparently likens the "steering module" of claim 30 to the network interfaces (Netmods) disclosed in *Desai*. The Netmods disclosed in *Desai* do not satisfy the claimed "steering module" because they do not provide a translate function that monitors each information communication provided to a first interface and a second interface, as required by claim 30. The disclosed Netmods only monitor packets provided to one interface, the Netmods themselves. *See, e.g., Desai*, 5:33-40 ("When a network data packet is then received on the assigned Netmod, the table is indexed to determine the assigned processing resource . . .). Because the Netmods disclosed by *Desai* only monitor packets provided to one interface – the Netmod itself – the Netmods disclosed by *Desai* do not satisfy the claimed "steering module . . . wherein the steering module provides a translate function that monitors each packet provided to said first interface and said second interface for packets to be provided malicious code analysis." It does not appear that the Office relies on *Muttik* to disclose this feature of claim 30, nor does it appear that *Muttik* discloses the claimed "steering module." Claim 30 is not obvious in view of the proposed combination of *Muttik* and *Desai* at least because the combination does not disclose the portion of claim 30 that recites "a steering module . . wherein said steering module provides a translate function that monitors each packet provided to said first interface and said second interface for packets."

ii. *The proposed combination does not teach or suggest a malicious code analyzer coupled to said steering module.*

Claim 30 is also not obvious in view of the proposed combination of *Muttik* and *Desai* because the proposed combination does not teaches or suggests a "malicious code analyzer coupled to said steering module for receiving packets . . . which are directed to said malicious code analyzer by said steering module . . . ." In fact, the Appellee, in rejecting claim 10, admits that *Muttik* does not disclose a steering module. Final Action, pg. 9. And *Desai* says nothing about malicious code analysis. Moreover, the Appellee has provided no evidence or explanation for why the claimed "malicious code analyzer coupled to said steering module" would have been obvious in view of *Muttik* and *Desai*.

iii. *The proposed combination does not disclose a malicious code analyzer coupled to a steering module for providing packets analyzed by the malicious code analyzer to the steering module*

Claim 30 also recites, in part, "said malicious code analyzer coupled to said steering module . . . for providing packets analyzed by said malicious code analyzer to said steering module." The Office has made no attempt to show where in the cited references – *Muttik* and *Desai* – this feature of claim 30 is disclosed. Moreover, the Office has not explained why this feature of claim 30 would have been obvious in view of *Muttik* and *Desai*.

iv. *The proposed combination does not teach a malicious code remediation function.*

Claim 30 recites, in part, "wherein said malicious code analyzer provides a malicious code remediation function." Neither *Muttik* nor *Desai* discloses this feature of claim 30. *Desai* is completely silent as to malicious code analysis. *Muttik* merely identifies potentially malicious code. The emulator disclosed by *Muttik* does not provide malicious code remediation. Claim 30 is not obvious in view of the proposed combination of *Muttik* and *Desai* the combination does not disclose a malicious code analyzer that "provides a malicious code remediation function."

v. *A person of ordinary skill would not have been motivated to make the proposed combination*

Claim 30 is also not obvious in view of the asserted combination because a person of ordinary skill would not have been motivated to make the proposed combination of *Muttik* and *Desai*. As discussed above, with respect to claims 13 and 20, the Office has not shown that a person of ordinary skill would have been motivated to combine *Muttik* and *Desai* to arrive at the claimed invention.

vi. *The Office has not articulated reasoning with some rational underpinning to support the legal conclusion of obviousness*

The Office has provided no explanation for why a person of ordinary skill would have found the invention of claim 30 obvious. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead;, there must be some articulated reasoning with some rational

underpinning to support the legal conclusion of obviousness."). As discussed above, there are significant differences between the claimed invention and the cited references – *Muttik* and *Desai*. The Office has offered no explanation for why it would have been obvious to modify and combine the teachings of *Muttik* and *Desai* to arrive at the claimed invention. For instance, the Appellee has offered no explanation for why the claimed "steering module" that "provides a translate function that monitors each packet provided to said first interface and said second interface" would have been obvious in view of *Desai* which provides a network interface (Netmod) that monitors only one interface. Further still, the Appellee has offered no explanation for how the network interface of *Desai* could have been coupled with the emulator of *Muttik*. Nor has the Appellee offered any explanation for why the claimed "malicious code remediation function" would have been obvious. The Appellee offered nothing more than conclusory statements in support of the rejection supported by no rational underpinning.

f. Dependent Claims 31-34 and 40-43

Claims 31-34 and 40-43 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Desai*. Dependent claims 31-34 and 40-43 each depend from independent claim 30 and inherit all of the limitations of claim 30. It has been shown above that *Muttik* in view of *Desai* does not meet the limitations of independent claim 30 and that a person of ordinary skill would not have been motivated to combine *Muttik* and *Desai*. The rejections of claims 31-34 and 40-43 do not cure the above identified deficiencies in the rejection of claim 30. Claims 31-34 and 40-43 are, therefore, allowable at least for their dependence from claim 30. Moreover, claims 31-34 and 40-43 recite features that make them patentable on their own.

i. Claim 31

Claim 31 recites "wherein said first interface is coupled to a network protected by said system and said second interface is coupled to a network not protected by said system." The Appellee argues that claim 31 has limitations similar to those of claims 20-22 and 26-29, and is rejected with the same rational applied against claims 20-22 and 26-29. But neither *Desai* nor *Muttik* disclose a system in which a first interface is coupled to a network protected by a system for providing protection against malicious code and a second interface is coupled to a network not protected by the system. Claim 31 is not obvious in view of the proposed

combination of *Muttik* and *Desai* at least because the asserted combination does not teach or suggest the claimed "wherein said first interface is coupled to a network protected by said system and said second interface is coupled to a network not protected by said system." In addition, the Office has provided no reason for why a person of skill in the art would have modified and combined *Muttik* and *Desai* to arrive at the claimed invention. The rejection of record simply cannot support a finding of obviousness. Appellant respectfully requests that the board reverse the rejection of claim 31.

ii. Claim 33

In the case of claim 33, the Office has once again ignored the claim language. The Office asserts that claim 33 has "limitations that [are] similar to those of claims 20-22 and 26-29, thus [it is] rejected with the same rationale applied against claims 20-22 and 26-29." Yet none of claims 20-22 and 26-29 claim a steering module that comprises "a frame store storing packets as received by said first interface and said second interface," as recited by claim 33.

Claim 33 is not obvious in view of the proposed combination of *Muttik* and *Desai* at least because neither reference teaches or suggest the portion of claim 33 that recites "wherein said first interface is coupled to a network protected by said system and said second interface is coupled to a network not protected by said system." Moreover, the Appellee has provided no reason for why a person of skill in the art would have modified and combined *Muttik* and *Desai* to arrive at the claimed invention. The rejection of record does not support a finding of obviousness. Accordingly, Appellant respectfully requests that the board reverse the rejection of record

4. The Rejections of Claims 2, 4-7, and 12 under 35 U.S.C. § 103 over *Muttik* in view of *Kouznetsov*, and further in view of *Mathon*

Claims 2, 4-7, and 12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Kouznetsov*, and further in view of *Mathon*. Final Action, pg. 12. Dependent claims 2, 4-7, and 12 depends directly from independent claim 1 and, thus, inherit all of the limitations of claim 1. The rejections of record do not rely on *Mathon* to cure the deficiencies of *Muttik* and *Kouznetsov* with respect to claim 1, nor does *Mathon* cure those deficiencies. It is respectfully submitted that dependent claims 2, 4-7, and 12 are allowable at least because of their dependence from claim 1 for the reasons discussed above.

Accordingly, Appellant respectfully requests that the Board reverse the rejection of claims 2, 4-7, and 12

Moreover, as will be discussed below, claims 2, 4-7, and 12 present subject matter that makes them patentable on their own. Further still, even if arguendo the proposed combination of *Muttik*, *Kouznetsov*, and *Mathon* disclosed every limitation of claims 2, 4-7, and 12, the Office has not satisfied its burden of showing that a person of ordinary skill would have been motivated to combine the three references to reach the claimed invention. As discussed above, a person of ordinary skill would not have been motivated to combine *Muttik* and *Kouznetsov*. The allegation that a person of ordinary skill would have been motivated to combine *Mathon* with *Muttik* and *Kouznetsov* is even more farfetched.

a. Dependent Claim 2

Claim 2 recites, in part, "said malicious code analyzer not having a network address associated therewith which is visible external to said system." The Office admits that neither *Muttik* nor *Kouznetsov* discloses this portion of claim 2. Final Action, pg. 12. The rejection of record relies on *Mathon*, at column 7, lines 1-10, as disclosing this portion of claim 2. Final Action, pg. 12. The Office's reliance on *Mathon* is misplaced. The cited portion of *Mathon* states, in part, that "[a]network connector appears to the outside world as a web proxy but only functions to deliver messages over message network 101." *Mathon*, 7:2-4 (emphasis added). According to *Mathon's* express disclosure, therefore, the disclosed network connectors are visible external to the network 101. Claim 2 is not obvious in view of *Muttik*, *Kouznetsov*, and *Desai* at least because the references do not disclose the portion of claim 2 that recites "said malicious code analyzer not having a network address associated therewith which is visible external to said system."

b. Claim 4

Claim 4 recites, in part, "a proxy for emulating a behavior of a destination of said information communication." The Office argues that the combination of *Mathon*, *Kousznetsov*, and *Muttik* disclose this portion of claim 4. Final action, pg. 13. Although the Office has not articulated why the aforementioned portion of claim 4 would have been obvious in view of *Mathon* and *Muttik*, it appears that the Office believes that claim 4 would have been obvious because *Mathon* uses the term "proxy" and *Muttik* discloses an emulator.

Even if the cited references taught or suggested every limitation of claim 4, which they do not, a person of ordinary skill would not have been motivated to make the proposed combination.

Mathon discloses network connectors for delivering messages over a business-to-business/electronic document interchange network. The cited portion of *Mathon* states that "[a] network connector appears to the outside world as a web proxy but only functions to deliver messages over message network 101." *Mathon*, 7:2-4. Thus, the network connectors of *Mathon*, which the Office apparently likens to the claimed "proxy," expressly teach away from the claimed "proxy for emulating a behavior of a destination of said information communication" because the disclosed network connector "only functions to deliver messages" over a message network. *Mathon*, 7:3-4. A person of ordinary skill would not, therefore, have been motivated to combine the teachings of *Muttik* and *Kouznetsov* with the teachings of *Mathon*, as proposed by the Office. *See, e.g., In re Grasselli*, 713 F.2d 731, 743 (Fed. Cir. 1983) (it is improper to combine references where the references teach away from their combination).

Moreover, the disclosed network connectors, which only function to deliver messages, cannot be modified to provide emulation without changing the network connectors' principle of operation. And it is well settled that a proposed modification of prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *See, e.g., In re Ratti*, 270 F.2d 810 (CCPA 1959); MPEP § 2143.01(VI) (2008).

c. Claim 5

Claim 5 recites "wherein said transparent configuration of said malicious code analyzer renders said proxy invisible to devices coupled to said system." The Office asserts that this portion of claim 5 is disclosed by *Mathon* – specifically, column 7, lines 1-10. Final Action, pg. 13. As an initial matter, the rejection of claim 5 does not specifically point out what elements disclosed by *Mathon* the Office believes satisfy the aforementioned portion of claim 5. Presumably the Office's position is that the disclosed network connectors meet the above-referenced portion of claim 5. Specifically, it appears that the Office has taken the position that *Mathon's* network based connectors are analogous to the claimed "proxy."

Yet nothing in the cited portion of *Mathon* suggests that the disclosed "network based connectors" are "invisible to devices coupled to said system." Rather, as discussed above, the disclosed network connects of *Mathon* "appear to the outside world as a web proxy." *Mathon*, 7:2-4. Mathon's network based connectors are, therefore, visible to devices coupled to the disclosed message network.

Moreover, the Office cites to the combination of *Muttik* and *Kouznetsov* as disclosing the claimed "malicious code analyzer" of claim 5. *See* Final Action, pg. 7 (alleging that the claimed "malicious code analyzer" is disclosed by *Muttik* and *Kouznetsov*). The Office has made no attempt to articulate how the combination of *Muttik* and *Kouznetsov* – the combination of which the Office likens to the claims "malicious code analyzer" – could possibly render the network connectors of *Mathon* invisible to devices coupled to the system.

Claim 5 is not obvious at least because the proposed combination of *Muttik*, *Kouznetsov*, and *Mathon* does not teach the portion of claim 5 that recites "wherein said transparent configuration of said malicious code analyzer renders said proxy invisible to devices coupled to said system." Moreover, the Appellee has made no attempt to articulate why a person of ordinary skill at the time of the invention would have found the claimed invention obvious in view of *Muttik*, *Kouznetsov*, and *Mathon*. Appellant respectfully requests that the Board reverse the rejection of claim 5.

d. Claim 6

Claim 6 recites, in part, "wherein said proxy comprises server functionality and client functionality." The Office points to *Mathon* as disclosing this portion of claim 6 – specifically, column 3, line 7, column 7, line 3, and column 9, lines 20-35. Final Action, pg. 13. The cited portion of column 3 discloses that electronic business transactions have adopted the central portal concept where customers use a browser to click into web pages resident on a server to conduct transaction. This portion of *Mathon* is part of the "Background of the Invention" and is completely unrelated to the disclosed network connectors, which the Office likens to the claimed "proxy." It appears that this portion of *Mathon* was cited because it uses the term "server." The cited portion of column 7 disclose that a network connector appears to the outside world as a web proxy. And the cited portion of column 9 merely summarizes security protocols available for connectors. The Appellee

has failed to provide any explanation for why these portions of *Mathon* are believed by the Appellee to meet the claimed proxy comprising server functionality and client functionality.

Nothing in *Mathon*, much less the cited portions, discloses that the network based connectors, which the Office apparently likens to the claimed "proxy," include server functionality and client functionality, as claimed by claim 6. As noted above, the disclosed network connectors appear to the outside world as a web proxy but only function to deliver messages over the disclosed message network. *Mathon*, 7:3-5. *Mathon*, therefore, teaches away from the claimed invention because the disclosed network connectors, which only function to deliver messages, are incapable of providing the claimed client and server functionality.

e. Claim 7

Claim 7 recites "a loop back interface for interfacing said information communication with said malicious code analyzer." The Office asserts that this portion of claim 7 is disclosed by *Muttik*, column 1 (lines 40-47), and *Mathon*, column 3 (line 35). The cited portion of *Muttik* merely discloses that a human can examine library code to determine whether a program is likely to exhibit malicious behavior. *Muttik*, 1:40-48. And the cited portion of *Mathon* merely discloses that the disclosed system "provides for a plurality of route point processors for routing messages independently of the internet service provider (ISPs) routers." The Appellee has failed to provide any evidence that the proposed combination of *Muttik*, *Kouznetsov*, and *Mathon* teach or suggest the claimed "loop back interface for interfacing said information communication with said malicious code analyzer." For at least this reason, claim 7 is not obvious. Appellant respectfully requests that the Board reverse the rejection of claim 7.

5. Rejections under 35 U.S.C. § 103(a) over *Muttik* in view of *Desai* and in further view of *Mathon*

Claims 15, 23-25, and 35-39 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Desai*, further in view of *Mathon*.

a. Claim 15

Dependent claims 15 depends from independent claim 13 and inherits all of the limitations of claim 13. It has been shown above that *Muttik* in view of *Desai* does not meet

the limitations of independent claim 13 and that a person of ordinary skill would not have been motivated to combine *Muttik* and *Desai*. The rejection of claim 15 does not cure the above identified deficiencies in the rejection of claim 13. Claim 15 is, therefore, allowable at least for their dependence from claim 13. Moreover, claim 15 recites features that make it patentable on its own.

According to the Office, claim 15 "has limitations that is [sic] similar to those of claim 6, thus it is rejected with the same rational applied against claim 6 above." As discussed above, with respect to claim 6, the network connectors of *Mathon*, which the Office likens to the claimed "proxy," do not comprise server and client functionality. The disclosed network connectors only function to deliver messages over the disclosed message network. *Mathon*, 7:3-5. For at least this reason the Office has failed to make a *prima facie* case of obviousness with respect to claim 15.

b. Claims 23-25

Dependent claims 23-25 each depend from independent claim 20 and inherit all of the limitations of claim 20. It has been shown above that *Muttik* in view of *Desai* does not meet the limitations of independent claim 20 and that a person of ordinary skill would not have been motivated to combine *Muttik* and *Desai*. The rejections of claims 23-25 do not cure the above identified deficiencies in the rejection of claim 20. Claims 23-25 are, therefore, allowable at least for their dependence from claim 20. Moreover, claims 23-25 recite features that make them patentable on their own.

For example, claim 23 recites "wherein said steering is accomplished in a manner which renders said malicious code analyzer invisible to said information communication originator and said intended recipient." The rejection of record states that claim 23 "has limitations that is [sic] similar to those of claim 5, thus it is rejected with the same rational applied against claim 6 above." Final Action, pg. 14. As an initial matter, Appellant disputes the Office's characterization of claim 23. Claim 5 recites "wherein said transparent configuration of said malicious code analyzer renders said proxy invisible to devices coupled to said system." Claim 23 recites "wherein said steering is accomplished in a manner which renders said malicious code analyzer invisible to said information communication originator and said intended recipient." Claims 5 and 23 clearly recite distinct subject matter.

Claim 23 is not obvious in view of the proposed combination of *Muttik*, *Desai*, and *Mathon* because none of the reference teach or suggest the claimed "wherein said steering is accomplished in a manner which renders said malicious code analyzer invisible to said information communication originator and said intended recipient." The Office apparently likens the "steering" of claim 23 to the message routing provided by the network connectors of *Mathon*. *See* Final Action, pp. 13-14 (rejections of claims 5 and 23). As discussed above, however, the network connectors disclosed by *Mathon* are visible to the outside world. *See Mathon*, 7:204 ("A network connector appears to the outside world as a web proxy . . . .").
Moreover, the disclosed *Mathon* does not teach or suggest that the disclosed network connectors do not render anything portion of the disclosed network invisible to an information communication originator and an intended recipient.

Moreover, the Office has provided no explanation for why or how a person of ordinary skill would have known methods to somehow modify a network connector in a business-to-business/electronic document interchange messaging network (*Mathon*) to render the claimed "malicious code analyzer" invisible. Claim 23 is not obvious because the proposed combination of *Muttik*, *Desai*, and *Mathon* does not disclose the portion of claim 23 that recites "wherein said steering is accomplished in a manner which renders said malicious code analyzer invisible to said information communication originator and said intended recipient" and the Office has not articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. Appellant respectfully requests that the Board reverse the rejection of claim 23.

c. Claims 35-39

Claims 35-39 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Muttik* in view of *Desai*, and further in view of *Mathon*. Final Action, pg. 14. Dependent claims 35-39 depend from independent claim 30 and, thus, inherit all of the limitations of claim 30. As shown above, the rejection of claim 30 in view of *Muttik* and *Desai* is deficient. The rejections do not rely on *Mathon* to cure the deficiencies of *Muttik* and *Desai* with respect to claim 30, nor does *Mathon* cure those deficiencies. Dependent claims 35-39 are allowable at least because of their dependence from claim 30 for the reasons discussed above.

i. Claim 35

Claim 35 recites "a proxy for emulating a behavior of a destination of ones of said packets." The rejection of claim 35 states that it is rejected based on the same rationale applied to claims 7 and 23-25. Final Action, pg. 15. As discussed above, *Mathon* teaches away from the proposed combination. The network connectors disclosed by *Mathon*, which the Office likens to the claimed "proxy" (see Final Action, pp. 13-14 (rejections of claims 4 and 7) only function to deliver messages. *Mathon*, 7:2-4. Thus, the disclosed network connectors of *Mathon* cannot be modified to emulate a behavior of a destination, as required by claim 35. Appellant respectfully requests that the Board reverse the rejection of claim 35.

ii. Claim 38

Claim 35 recites "a proxy for emulating a behavior of a destination of ones of said packets." The Appellee asserts that claim 38 is rejected based on the same rationale applied in rejecting claims 7 and 23-25. Final Action, pg. 15. But none of claims 7 or 23-25 claim recite "wherein said proxy communicates with said steering module using a network stack." The Office has, therefore, failed to make a *prima facie* case of office by failing to compare the claim language to the prior art. *See Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). Moreover, the Office has failed to articulate a rational basis for why a person of ordinary skill would have found the claimed invention obvious based on the teachings of *Muttik*, *Desai*, and *Mathon*. The Office offers nothing more than a conclusory statements, which are insufficient to support a finding of obviousness. Appellant respectfully requests that the Board reverse the rejection of claim 38.

VIII. CLAIMS APPENDIX

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Appellee is being submitted.

X. RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced in II. above, hence copies of decisions in related proceedings are not provided.

In view of the foregoing, Appellant respectfully requests withdrawal of the final rejection, reopening of prosecution, and allowance of the above-captioned application. Should Appellee not find the comments contained herein persuasive, acknowledgement of receipt and entry of this Appeal brief are respectfully requested.

CONCLUSION

Appellant believes that a fee of $270.00 is due with the Appeal brief and is being paid by credit card. However, if there are any additional fees due, please charge our Deposit Account No. 06-2380, under Order No. 58895/P003US/10305848 during the pendency of this Application pursuant to 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Dated: March 31, 2009

Respectfully submitted,

By_____
Thomas Kelton
Registration No.: 54,214
FULBRIGHT & JAWORSKI L.L.P.
2200 Ross Avenue, Suite 2800
Dallas, Texas 75201-2784
(214) 855-7115
(214) 855-8200 (Fax)
Attorney for Appellant

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the U. S. Patent and Trademark Office electronic filing system in accordance with § 1.6(a)(4).

By: 
Linda L. Gibson

Date of Transmission: March 31, 2009

APPENDIX A

1. A system for providing protection against malicious code, said system comprising:

a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient of said information communication to intercept said information communication and to analyze said information communication for malicious code, said malicious code analyzer being configured to be transparent to systems of said communication system.

2. The system of claim 1, wherein said transparent configuration of said malicious code analyzer comprises said malicious code analyzer not having a network address associated therewith which is visible external to said system.

3. The system of claim 1, wherein said transparent configuration of said malicious code analyzer comprises:

a translate function that monitors each packet provided to an interface of said system for packets to be provided malicious code analysis by said malicious code analyzer.

4. The system of claim 1, wherein said malicious code analyzer comprises:

a proxy for emulating a behavior of a destination of said information communication.

5. The system of claim 4, wherein said transparent configuration of said malicious code analyzer renders said proxy invisible to devices coupled to said system.

6. The system of claim 4, wherein said proxy comprises:

server functionality; and

client functionality.

7. The system of claim 4, further comprising:

a loop back interface for interfacing said information communication with said malicious code analyzer.

8. The system of claim 1, wherein said malicious code analyzer comprises:

code for virus scanning.

9. The system of claim 1, wherein said malicious code analyzer comprises:

code for identifying unwanted or unsolicited messages.

10. The system of claim 1, further comprising:

a steering module for said information communication between a first interface and a second interface of said system, wherein said steering module provides a translate function that monitors each information communication provided to said first interface and said second interface for information communication to be provided malicious code analysis and directs at least some of said information communication to said malicious code analyzer.

11. The system of claim 1, further comprising:

a communications throttle for determining if said information communication is to be passed by said system.

12. The system of claim 1, wherein said information communication conforms to a protocol selected from the group consisting of:

simple mail transfer protocol (SMTP);

post office protocol (POP);

hypertext transfer protocol (HTTP);

Internet message access protocol (IMAP);

file transfer protocol (FTP);

domain name service (DNS);

hot standby router protocol (HSRP);

open shortest path first (OSPF); and

enhanced interior gateway routing protocol (EIGRP).

13. A computer program product having a computer readable medium having computer program logic recorded thereon for providing protection against malicious code, said computer program product comprising:

code for analyzing malicious code present in information communication traffic between an originator of an information communication of said communication traffic and an intended recipient of said information communication; and

code for a steering said information communication between interfaces associated with said information communication originator and said intended recipient and providing a translate function which detours at least a portion of said information communication to said code for analyzing malicious code and which renders said code for analyzing malicious code invisible to said information communication originator and said intended recipient.

14. The computer program product of claim 13, further comprising:

proxy code interfacing said information communication with said code for analyzing malicious code.

15. The computer program product of claim 14, wherein said proxy code comprises server and client functionality.

16. The computer program product of claim 13, wherein said code for analyzing malicious code comprises virus scanning code.

17. The computer program product of claim 13, wherein said code for analyzing malicious code comprises undesired or unsolicited message identification code.

18. The computer program product of claim 13, wherein said translate function monitors each information communication provided to a first interface of said interfaces and a second interface of said interfaces for information communication to be provided malicious code analysis.

19. The computer program product of claim 13, further comprising:

code for throttling communications by receiving information with respect to information communication and determining if said information communication is to be passed by said interfaces.

20. A method for providing protection against malicious code, said method comprising:

intercepting packets in an information communication traffic pattern;

steering said packets between interfaces associated with an information communication originator and said intended recipient, said steering providing detouring of at least a portion of said packets to a malicious code analyzer; and

analyzing said at least a portion of said packets by said malicious code analyzer before releasing said at least a portion of said packets back into said traffic pattern.

21. The method of claim 20, further comprising:

disposing a protective system providing said intercepting, steering, and analyzing in a network link between said information communication originator and said intended recipient.

22. The method of claim 21, wherein said protective system is disposed as a protected network edge device.

23. The method of claim 20, wherein said steering is accomplished in a manner which renders said malicious code analyzer invisible to said information communication originator and said intended recipient.

24. The method of claim 20, further comprising:

interfacing said information communication with said code for analyzing malicious code using a proxy.

25. The method of claim 21, wherein said proxy comprises a proxy server and a proxy client.

26. The method of claim 20, wherein said analyzing said at lest a portion of said packets comprises:

scanning for viruses.

27. The method of claim 20, wherein said analyzing said at least a portion of said packets comprises:

identifying undesired or unsolicited messages.

28. The method of claim 20, wherein said steering comprises:

monitoring each packet provided to a first interface and a second interface for information communication to be provided malicious code analysis.

29. The method of claim 20, further comprising:

throttling communications by receiving information with respect to said packets and determining if said packets are to be passed in said traffic pattern.

30. A system for providing protection against malicious code, said system comprising:

a steering module for directing packets between a first interface and a second interface of said system, wherein said steering module provides a translate function that monitors each packet provided to said first interface and said second interface for packets to be provided malicious code analysis and directs at least some of said packets to a malicious code analyzer; and

said malicious code analyzer coupled to said steering module for receiving packets which are not addressed for receipt by said malicious code analyzer but which are directed to said malicious code analyzer by said steering module and for providing packets analyzed by said malicious code analyzer to said steering module, wherein said malicious code analyzer provides a malicious code remediation function.

31. The system of claim 30, wherein said first interface is coupled to a network protected by said system and said second interface is coupled to a network not protected by said system.

32. The system of claim 31, wherein said system is disposed at an edge of said protected network.

33. The system of claim 30, wherein said steering module comprises:

a frame store storing packets as received by said first interface and said second interface.

34. The system of claim 30, wherein said steering module comprises:

a station map providing information with respect to which of said first interface and said second interface particular destinations of said packets are coupled to.

35. The system of claim 30, wherein said malicious code analyzer comprises:

a proxy for emulating a behavior of a destination of ones of said packets.

36. The system of claim 35, wherein said translate function of said steering module renders said proxy invisible to devices coupled to said first interface and said second interface.

37. The system of claim 35, wherein said proxy comprises:

a proxy server; and

a proxy client.

38. The system of claim 35, wherein said proxy communicates with said steering module using a network stack.

39. The system of claim 38, wherein said proxy communicates with said steering module using said network stack through use of a loop back interface.

40. The system of claim 30, wherein said malicious code analyzer comprises:

code for virus scanning.

41. The system of claim 40, wherein said code for virus scanning comprises:

commercially available virus scanning software integrated into said malicious code analyzer.

42. The system of claim 30, wherein said malicious code analyzer comprises:

code for identifying unwanted or unsolicited messages.

43. The system of claim 30, further comprising:

a communications throttle coupled to said steering module for receiving information with respect to packets which are not addressed for receipt by said communications throttle but which information with respect thereto is directed to said communications throttle by said steering module and for determining if said packets are to be passed by said system.

APPENDIX B

NONE

APPENDIX C

NONE